REMARKS

Claims 1-26 are presented for examination. Claims 4 and 11 have been amended to define more clearly what Applicant regards as his invention. Claims 1, 4, 8, and 11 are in independent form. Favorable reconsideration is requested.

Claims 1, 3, 8, 10, 17-19, and 22 were rejected under 35 U.S.C. § 103(a) as being obvious from Cox et al. (U.S. Patent 5,915,027) in view of Moskowitz et al. (U.S. Patent 5,889,868); Claims 2 and 9, as being obvious from Cox et al. in view of Moskowitz et al., and further in view of Sandford, II et al. (U.S. Patent 5,727,092); Claim 15, as being obvious from Cox et al. in view of Moskowitz et al., and further in view of Kunimoto et al. (U.S. Patent 5,303,236); Claims 20 and 21, as being obvious from Cox et al. in view of Moskowitz et al., and further in view of Mahe (U.S. Patent 6,459,685); Claims 4-7, 11-14, 17, 18, 23, and 26, as being obvious from Cox et al. in view of Nakagawa et al. (U.S. Patent 6,104,826); Claim 16, as being obvious from Cox et al. in view of Nakagawa et al., and further in view of Kunimoto et al.; and Claims 24 and 25, as being obvious from Cox et al. in view of Nakagawa et al., and further in view of Mahe.

Claim 1 is directed to a method of inserting a message into digital data representative of physical quantities, the message including ordered symbols. The method includes the steps of segmenting the data into regions, and associating at least one region with each symbol to be inserted. For each region into which a symbol in question is to be inserted, the associating step includes the steps of (1) determining a pseudo-random function, from a key which depends on an initial key and on a length of the message, (2) modulating the symbol in question by a previously determined pseudo-random function in

order to supply a pseudo-random sequence, and (3) adding the pseudo-random sequence to a region in question.

One notable feature of Claim 1 is determining a pseudo-random function from a key which depends on an initial key and on a length of the message.

Cox et al., as understood by Applicant, relates to relates to digital watermarking and discusses a watermark insertion and extraction processes. The Examiner concedes at page 4 of the Office Action that Cox et al. "does not disclose means for determining a pseudo-random function, for each region into which a symbol is to be inserted, from a key which depends on an initial key and on a length of the message." However the Examiner asserts (see, e.g., page 2 of the Office Action) that Moskowitz et al. "does disclose determining a pseudo-random function from a key which depends on an initial key and on a length of the message (Column 17, lines 9-31; and Column 18, line 30 to Column 19, line 32)."

Moskowitz et al., as understood by Applicant, relates to optimization methods for the insertion, protection, and detection of digital watermarks in digitized data. Applicant, however, is unable to agree with the Examiner's analysis, for the following reasons.

First, in the cited portion of Moskowitz et al. (column 17, lines 9-31), Moskowitz et al. alludes to message length merely for being potentially important to the security of the watermarking scheme. Specifically, that portion of Moskowitz et al. states:

> With digital watermarks, descriptive analysis of an information signal is important to preanalyze a given watermark's noise signature. Analysis of this signature versus the preanalysis of the target content signal for optimized insertion location and key/message length, are potentially important components to the overall implementation of the secure watermark. (Column 17, lines 9-14.)

Moskowitz et al. does not teach or suggest the determination of a pseudo-random function from a key which depends notably on a length of the message, as recited in Claim 1.

Referring also to the portion of Moskowitz et al. at column 7, lines 29-62 (cited by the Examiner at page 4 of the Office Action), and as explained in the Amendment filed on May 4, 2005, Moskowitz et al. merely discusses that, when actually implementing a known watermarking scheme with a fixed message length, the choice of the length of the message is made by the designing engineer according to the general rules as set forth in column 7, lines 57-62. These general concerns cannot fairly be considered a description of a way to generate a pseudo-random sequence, let alone the use of the length of the message to determine a pseudo-random function. Accordingly, Moskowitz et al. does not teach or suggest the determination of a pseudo-random function from a key which depends notably on a length of the message, as recited in Claim 1.

Moskowitz et al. also mentions the length of the message in column 17, as follows:

> Each instance of a watermark, where many are added to a given content signal given the size of the content and the size of the watermark message, can be "noise shaped" and the binary description of the watermark signature may be made unique by hashing" the data that comprises the watermark.

This is merely a statement that many watermarks may be added to a given content signal given the size of the content and the size of the watermarked message, and the cited portion of Moskowitz et al. does not therefore contain any teaching or suggestion of how a pseudo-random function should be determined. Accordingly, the portion of column 17 of Moskowitz et al., cited by the Examiner, clearly fails to teach or suggest the determination of a pseudo-random function from a key which depends notably on a length of the message, as recited in Claim 1.

In the portion of Moskowitz et al. from column 18, line 30, to column 19, line 32, also cited by the Examiner, Moskowitz et al. proposes to vary the algorithm used to embed and extract the watermark. However, Moskowitz et al. proposes only two ways for varying the algorithm. The first way is based on the "characteristics of the signal stream" (see column 18, lines 35-37 and lines 59-60 of that patent), i.e., according to the data to be watermarked, not to the message to be inserted, in order to adapt the algorithm used for the processed data. The second way is randomly, based on the pseudo-random key – again, not on the length of the message – for increased security (see column 18, lines 48-54, and column 19, lines 7-14 of that patent).

Therefore, the portion of Moskowitz et al. from column 18, line 30, to column 19, line 32, also fails to teach or suggest the determination of a pseudo-random

function from a key which depends notably on the length of the message, as recited in Claim 1.

For all of these reasons, nothing in Cox et al. or Moskowitz et al., whether considered separately or in any permissible combination (if any) would teach or suggest the determination of a pseudo-random function from a key which depends notably on a length of the message, as recited in Claim 1.

Accordingly, Claim 1 is seen to be clearly allowable over Cox et al. and Moskowitz et al., whether considered either separately or in any permissible combination (if any).

Independent Claim 8 is a device claim corresponding to method Claim 1, and is believed to be patentable over Cox et al. and Moskowitz et al. for at least the same reasons as discussed above in connection with Claim 1.

Claim 4 is directed to a method for extracting a message from digital data representative of physical quantities, the message including ordered symbols. The method includes the steps of segmenting the data into regions, extracting a length of an inserted message based on the digital data, and extracting the inserted message.

One notable feature of Claim 4 is extracting a length of an inserted message based on the digital data.

The Examiner cites column 9, line 21, to column 10, line 3, of Cox et al., as allegedly showing means for extracting a length of the inserted message. In particular, the Examiner states the following at page 2 of the Office Action:

> Cox does disclose extracting a length of the inserted message via breaking down the image into a set of subimages that are each of the same size (Column 9, line 61 to Column 10, line 3). The length of the inserted message is dependent upon, and determined by, the amount of subimages that are contained within the original image.

Thus, the Examiner appears to consider that, in Cox et al., the length of the inserted message is extracted when an image is broken down into blocks of a fixed size and the number of blocks thereby determined.

In the method of Claim 4, a length of an inserted message is extracted based on the digital data. That is, the length of the inserted message is extracted from the data itself. As noted above, the Examiner states regarding Cox et al. that "the length of the inserted message is dependent upon, and determined by, the amount of subimages that are contained within the original image", not based on the data itself, as recited in Claim 4. Cox et al. therefore fails to teach or suggest that the length of the message could be contained in the data itself.

Nothing in Cox et al. would teach or suggest extracting a length of an inserted message based on the digital data, as recited in Claim 4.

Nakagawa et al., as understood by Applicant, relates to watermark-embedding/extracting identification information into/from picture data. However, nothing has been found in Nakagawa et al. that would remedy the deficiencies of Cox et al. discussed above. This is because, in Nakagawa et al., the length L of the inserted message is predetermined; as is clearly understood from the description of the extraction process

(see column 13 of that patent, cited by the Examiner), there is no determination of the length L before the extraction of the "L-Piece weight coefficient". Nakagawa et al. does not propose, therefore, any step of extracting a length of an inserted message, let alone its determination based on the processed data, as in Claim 4.

Nothing in Cox et al. or Nakagawa et al., whether considered separately or in any permissible combination (if any) would teach or suggest extracting a length of an inserted message based on the digital data, as recited in Claim 4.

Accordingly, Claim 4 is seen to be clearly allowable over Cox et al. and Nakagawa et al., whether considered separately or in any permissible combination (if any).

Independent Claim 11 is a device claim corresponding to method Claim 4, and is believed to be patentable over Cox et al. and Nakagawa et al. for at least the same reasons as discussed above in connection with Claim 4.

A review of the other art of record has failed to reveal anything which, in Applicant's opinion, would remedy the deficiencies of the art discussed above, as references against the independent claims herein. Those claims are therefore believed patentable over the art of record.

The other claims in this application are each dependent from one or another of the independent claims discussed above and are therefore believed patentable for the same reasons. Since each dependent claim is also deemed to define an additional aspect of the invention, however, the individual reconsideration of the patentability of each on its own merits is respectfully requested.

In view of the foregoing amendments and remarks, Applicant respectfully requests favorable reconsideration and early passage to issue of the present application.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should continue to be directed to our below listed address.

Respectfully submitted,

Raymond A. DiPerna

Raymond A. DiPerna
Attorney for Applicant
Registration No.: 44,063

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200